ON THE TOTALITY OF THE SUBSTITUTIONS ON n LETTERS WHICH ARE COMMUTATIVE WITH EVERY SUBSTITUTION OF A GIVEN GROUP ON THE SAME LETTERS.

By G. A. MILLER.

(*Read April 20, 1911.*)

§ 1. Introduction.

The problem to determine all the substitutions on n letters which are commutative with every substitution of a regular group on the same letters was first solved explicitly by Jordan in his thesis. It was found that with every regular group there is associated a group which is conjugate with this regular group, such that each is composed of all the substitutions which are commutative with every substitution of the other.[1] These two regular groups were called *conjoints* by Jordan and it is evident that they have a common holomorph and that their group of isomorphisms is the quotient group of this holomorph with respect to either of these two regular groups.

The more general problem to determine all the substitutions on n letters which are commutative with every substitution of any transitive group on the same letters seems to have been solved for the first time by Kuhn in his thesis.[2] He found that with each transitive group G of degree n there is associated a group K on the same n letters which is composed of regular substitutions on these n letters, in addition to the identity. The order of K is α, the degree of the subgroup composed of all the substitutions of G which omit a given letter being $n - \alpha$. Hence a necessary and sufficient condition that K be transitive is that G be regular, and the number of the systems of intransitivity of K is always equal to n/α. When $\alpha < n$ K is formed by establishing a simple isomorphism between n/α

[1] Jordan, thesis, Paris, 1860, p. 39.

[2] Kuhn, *American Journal of Mathematics*, Vol. 26, 1904, p. 67.

regular groups, each of these regular constituent groups being transformed into every other under G. In particular, the degrees of these separate regular groups are systems of imprimitivity of G.

While K is composed of all the substitutions on these letters which are commutative with every substitution of G it is not generally true that G is also composed of all the substitutions which are commutative with every substitution of K and involve only the letters of K. It is evident that a necessary and sufficient condition that such reciprocal relations should exist between G and K is that G involves as an invariant subgroup the direct product of n/α regular groups, and that the remaining substitutions of G permute these regular groups according to the symmetric group of degree n/α. The order of G must therefore be

$$\alpha^k \cdot k!, \quad \text{where} \quad k = n/\alpha.$$

Hence the theorem: *A necessary and sufficient condition that a transitive group G of degree n involve all the substitutions on these n letters which are commutative with every substitution of the group K composed of all the substitutions on these n letters which are commutative with every substitution of G, is that the order of G be $\alpha^k \cdot k!$, where the degree of the subgroup of G which is composed of all its substitutions which omit a given letter is $n - \alpha$ and $k = n/\alpha$.*

When G does not include all the substitutions which are commutative with every substitution of K it is clearly a subgroup of the group formed by such substitutions. Hence we have the theorem: *If a transitive group of degree n is such that a subgroup composed of all its substitutions which omit a given letter is of degree $n - \alpha$ the order of this transitive group must divide $\alpha^k \cdot k!$, where $k = n/\alpha$.* To illustrate this theorem as well as the theorem of the preceding paragraph we may use for G the group of the square represented as a substitution group on four letters. In this case $\alpha = 2$, $k = 2$, and the order of G is exactly $\alpha^k \cdot k!$ Moreover, K is of order 2, and of degree 4, and G includes all the substitutions on these four letters which are commutative with every substitution of K, so that G and K are so related that each is composed of all the substitutions on

these letters which are commutative with every substitution of the other. A necessary and sufficient condition that K be a subgroup of G, when G and K are so related that each is composed of all the substitutions on these letters which are commutative with every substitution of the other, is that K be abelian. When G and K are both abelian they must be regular and identical.

It may be of interest to consider several of the special cases of the general theorems expressed above. When $\alpha = 1$, K is the identity. That is, if the subgroup, composed of all the substitutions which omit a given letter of a transitive group of degree n, is of degree $n-1$ the identity is the only substitution on these n letters which is commutative with every substitution of this transitive group, and the order of this group divides $n!$ In the other extreme case, when $\alpha = n$, the given theorems include the main known results as regards the substitutions which are commutative with every substitution of a regular group. As the term conjoints has an established meaning as regards regular groups it seems undesirable to use this term with the more general meaning that each of two substitutions groups of degree n is composed of all the substitutions on these n letters which are commutative with every substitution of the other. We shall therefore call such groups *amicable*, using a term of Greek number theory. Hence we may say that a necessary and sufficient condition that a transitive group of degree n is one of a pair of amicable groups is that its order be $\alpha^k \cdot k!$, $n - \alpha$ being the degree of one of its subgroups composed of all its substitutions which omit a given letter, and $k = n/\alpha$. This proves also incidentally that n is always divisible by α.

From the preceding results it is easy to deduce a theorem as regards the total number of the transitive groups of degree n which belong to pairs of amicable groups. In fact, since K is composed of simply isomorphic regular groups the number of the distinct possible groups K is equal to the number of the different abstract groups of order α, two substitution groups being regarded as distinct only when it is not possible to transform one into the other. As G is completely determined by K there results the following theorem: *The number of the distinct transitive groups of degree n which*

belong to pairs of amicable groups is equal to the sum of the numbers of the abstract groups whose orders are divisors of n, including n and unity among these divisors.

§ 2. Amicable Intransitive Groups.

In the preceding section it was observed that a necessary and sufficient condition that each of two amicable groups be transitive is that they be regular, and that if a non-regular transitive group belongs to a pair of amicable groups the second group of the pair is intransitive. It remains to consider the case when each one of a pair of amicable groups is intransitive. An infinite system of such groups may be constructed by establishing a simple isomorphism between n symmetric groups of degree n, $n > 2$, and determining the totality of the substitutions which are commutative with every substitution of the intransitive group G thus formed. It is evident that this totality of substitutions constitutes a group K which is similar to G. That is, G and K are two conjugate intransitive substitution groups each being composed of all the substitutions on these n^2 letters which are commutative with every substitution of the other.

The existence of the two amicable intransitive groups G and K of the preceding paragraph may also be established as follows: Consider the n^2 m-sets[1] of the symmetric group of degree n as regards the symmetric group of degree $n - 1$. On multiplying these n^2 m-sets on the right by all the substitutions of this symmetric group the n^2 m-sets are permuted according to a group G' similar to G, and by multiplying them on the left they are permuted according to a similar group K'. From the fact that multiplication is associative it results that every substitution of G' is commutative with every substitution of K'. Moreover as every substitution on these n^2 letters which is commutative with every substitution of G' must permute some of its systems, it is evident that K' is composed of all the substitutions on these letters which are commutative with every substitution of G', and vice versa; that is, G' and K' are in fact two amicable intransitive groups for every value of n. The group

[1] If H is any subgroup of a group G, the total number of distinct sets of operators of the form $S_\alpha H S_\beta$, where S_α and S_β are operators of G, are known as the m sets of G as regards H.

generated by G' and K' is clearly imprimitive and of order $(n!)^2$.

The existence of amicable intransitive groups which are not included in the preceding infinite system can be easily proved by the following examples: Let G be the dihedral group of order 8 and H any one of its non-invariant subgroups of order 2. With respect to H there are 8 m-sets of G since H is transformed into itself by 4 of the operators of G. Hence these eight m-sets are permuted according to a group which is simply isomorphic with G and has two transitive constituents both by right and also by left multiplication. Each of the two substitution groups obtained in this way is clearly composed of all the substitutions on these eight letters which are commutative with every substitution of the other and hence these are two amicable intransitive groups whose transitive constituents are not symmetric.

The substitutions which are commutative with every substitution of an intransitive group G either interchange systems of intransitivity, or they are composed of constituents which are separately commutative with the various transitive constituents of G. The latter have been considered in the preceding section. Hence we shall, for the present, confine our attention to those substitutions which are commutative with every substitution of G and interchange its systems of intransitivity. It is evident that these systems of intransitivity are transformed by all the substitutions which are commutative with every substitution of G according to a substitution group, and that those transitive constituents of G which are transformed transitively among themselves must be simply isomorphic in G. These constituents are clearly transformed according to a symmetric group by all the substitutions which are commutative with every substitution of G. Hence the theorem: *If an intransitive group G is one of a pair of amicable intransitive groups, and if the transitive constituents of G are such that no substitution on the letters of the separate constituents is commutative with every substitution of the constituent, then must the consituents of G be symmetric groups.*

It is clear that G may have more than one set of transitive constituents such that all those of a set are conjugate under the totality

of the substitutions K which are commutative with every substitution of G. In other words, the substitution group according to which the transitive constituents of G are transformed may be intransitive. When this condition is satisfied K is the direct product of two or more symmetric groups. This suggests a more general infinite system of pairs of amicable intransitive groups than the one mentioned above: viz., Let G be the direct product of the ρ groups formed by establishing simple isomorphisms between n_1 symmetric groups of degree n_1, n_2 symmetric groups of degree n_2, $\cdots$, n_ρ symmetric groups of degree n_ρ (n_1, n_2, $\cdots$, n_ρ being distinct numbers greater than 2), it is clear from what was proved above that K is similar to G and hence G and K are amicable intransitive groups. It should be observed that G and K are *always amicable whenever they are similar* but that the converse of this theorem is not always true. This more general system of amicable intransitive groups may clearly be constructed by forming the direct product of the ρ symmetric groups of degrees n_1, n_2, $\cdots$, n_ρ respectively and forming the m-sets as regards the subgroups H obtained by forming the direct product of ρ symmetric groups of degrees $n_1 - 1$, $n_2 - 1$, $\cdots$, $n_\rho - 1$ respectively, one being taken from each of the given symmetric groups, in order. If the m-sets thus obtained are multiplied on the right and on the left by all the operators of these sets there clearly results the two systems of amicable intransitive groups in question.

To obtain a still more general infinite system of amicable intransitive groups it should be first observed that the intransitive group formed by establishing a simple isomorphism between m_1 symmetric groups of degree n_1, written on m_1 distinct sets of letters, is amicable with the one obtained by establishing a simple isomorphism between n_1 symmetric groups of degree m_1, written on n_1 distinct sets of letters, where n_1, $m_1 > 2$. Hence it results that the direct product formed by multiplying ρ intransitive groups of degrees $n_1 m_1$, $n_2 m_2$, $\cdots$, $n_\rho m_\rho$ respectively, each being formed in the former of the two ways mentioned above, is amicable with the direct product formed by multiplying the ρ groups of the same degrees respectively, but constructed by establishing a simple isomorphism between n_1 sym-

metric groups of degree m_1, n_2 of degree m_2, $\cdots$, n_ρ of degree m_ρ respectively. Moreover, it results from the given theorem that these direct products include all the possible sets of amicable groups in which each of the two groups is intransitive and each of the transitive constituents is not commutative with any substitution besides the identity on the letters of the constituent.

The above therefore completes the determination of amicable groups when both groups are intransitive, and the transitive constituents are such as to involve subgroups whose degrees are just one less than the degrees of the respective constituents. The cases in which at least one of the two amicable groups is transitive were considered in the introduction. It may be observed that whenever an intransitive group is formed by establishing a simple isomorphism between more than two symmetric groups it is one of a pair of amicable groups. The second group is transitive when each of these symmetric groups is of degree 2, when this condition is not satisfied the second group is also a simple isomorphism between symmetric groups. The group obtained by establishing a simple isomorphism between two symmetric groups is evidently never one of a pair of amicable groups unless the two symmetric groups are of order 2. We may express this result in the form of a theorem as follows: *The intransitive group G formed by establishing a simple isomorphism between three or more symmetric groups, written on distinct sets of letters, is one of a pair of amicable groups, the second group K being also such an intransitive group whenever the degree of the given symmetric groups exceeds 2. The intransitive group formed by establishing a simple isomorphism between two symmetric groups is one of two amicable groups only in the special case when these symmetric groups are of degree 2.*

By means of the given results it is not difficult to complete the determination of all possible pairs of amicable intransitive groups. Suppose that G is constructed by establishing a simple isomorphism between any number of conjugate transitive groups written on distinct letters, each constituent being one of a pair of amicable groups. If these constituents are not symmetric and not regular it is clear that G is one of a pair of amicable groups and that the number of the

transitive constituents of K is equal to the number of transitive constituents in the amicable group corresponding to a transitive constituent of G. Moreover, G is evidently not one of a pair of amicable groups when its constituents do not have this property. Hence there results the theorem: *Two necessary and sufficient conditions that a given intransitive group be one of a pair of amicable groups are:* 1) *that it be the direct product of transitive constituents which belong to pairs of amicable groups, or of sets of simply isomorphic transitive constituents of this kind, or* 2) *that the number of simply isomorphic constituents be greater than two whenever they are symmetric but not regular.* From the Introduction it results that the second group of this pair is also intransitive except in the case when the intransitive group is composed of simply isomorphic regular groups. It reduces to the identity whenever the given intransitive group is the direct product of symmetric groups whose degrees exceed 2. The pair of amicable groups are conjugate whenever one is the direct product of regular groups, of sets of m simply isomorphic non-regular symmetric groups of degree n if the m's and n's may be put into (1, 1) correspondence such that the corresponding pairs are equal, or of sets of m simply isomorphic non-symmetric transitive groups of degree n ($n - \alpha$ being the degree of a subgroup composed of all the substitutions of the constituent which omit a letter) if the α's, m's and n/α's may be put into (1, 1) correspondence such that the corresponding triplets may be α, n/α, αm for every set of values α, m, n.

University of Illinois.